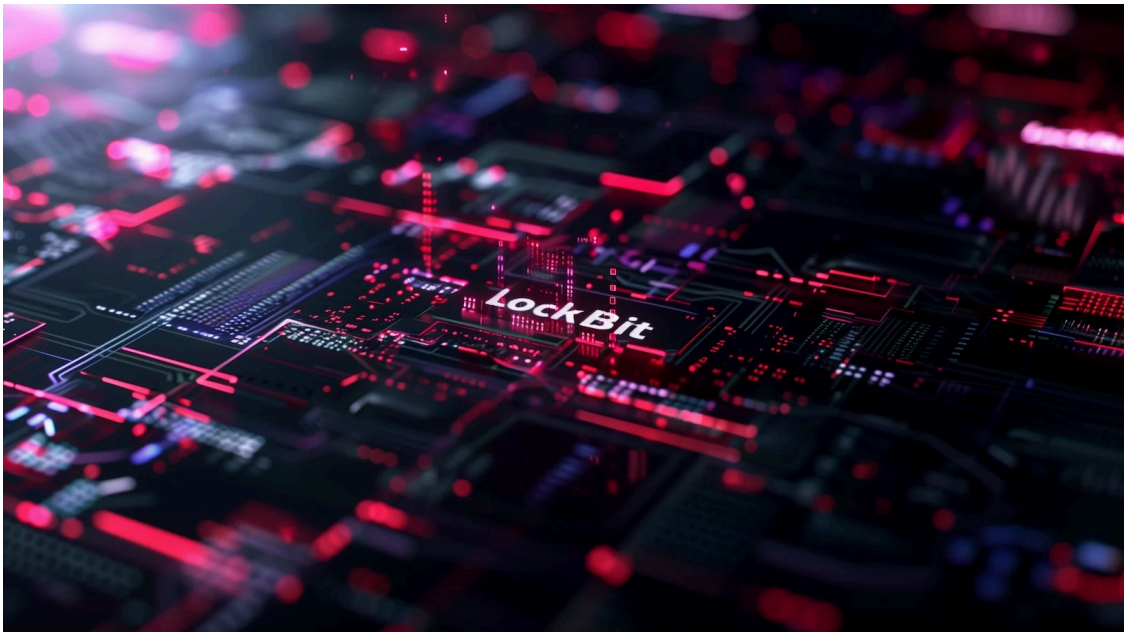
LockBit ransomware returns, restores servers after police disruption

By Ionut Ilascu

Published: 2024-02-25 · Archived: 2026-04-05 18:34:24 UTC

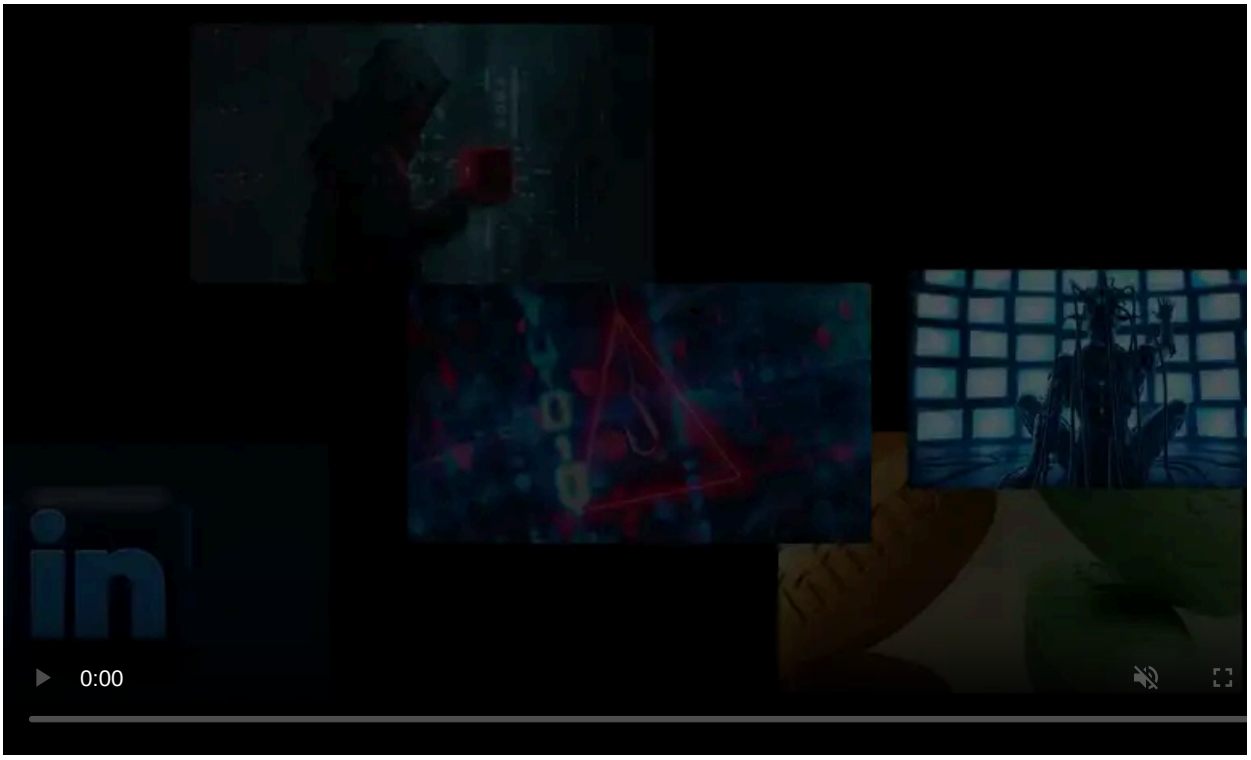


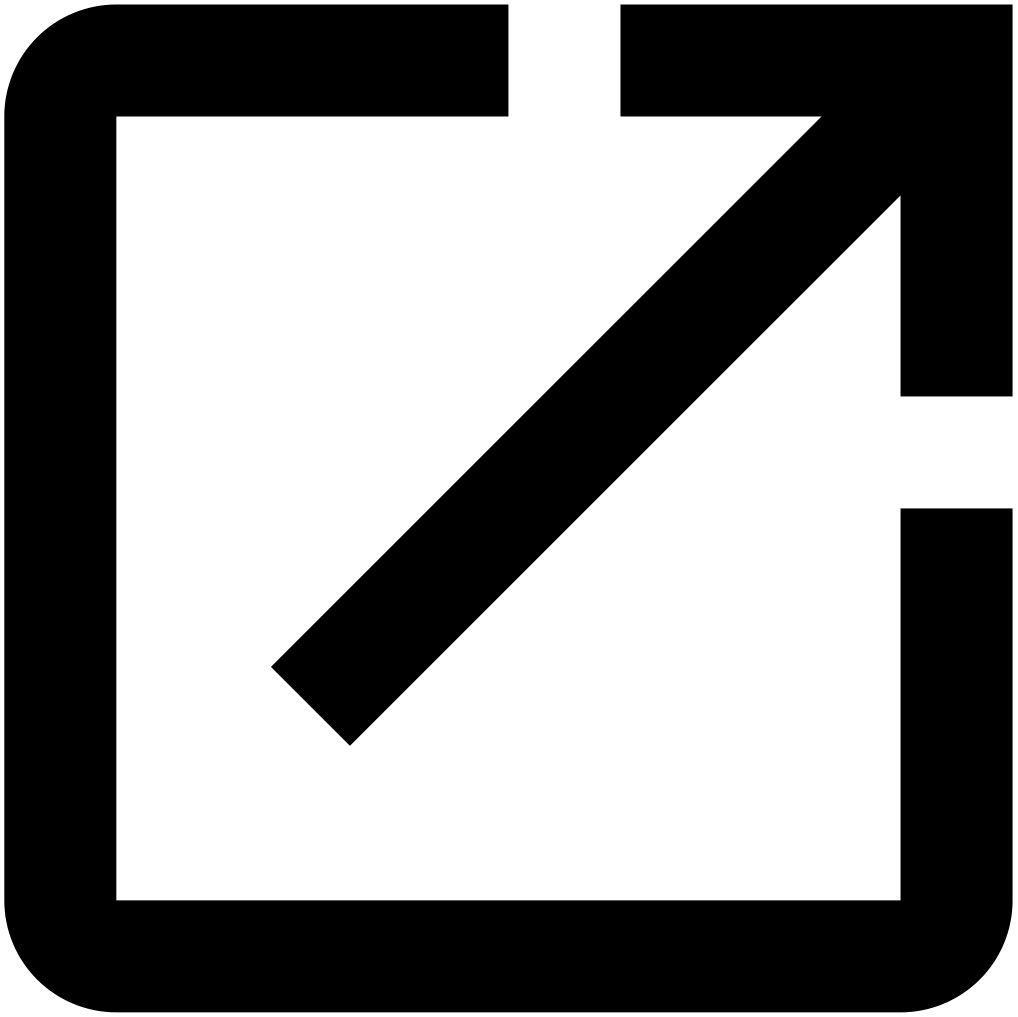
The LockBit gang is relaunching its ransomware operation on a new infrastructure less than a week after law enforcement hacked their servers, and is threatening to focus more of their attacks on the government sector.

In a message under a mock-up FBI leak - specifically to draw attention, the gang published a lengthy message about their negligence enabling the breach and the plans for the operation going forward.

LockBit ransomware continues attacks

On February 19, authorities took down LockBit's infrastructure, which included 34 servers hosting the data leak website and its mirrors, data stolen from the victims, cryptocurrency addresses, decryption keys, and the affiliate panel.


0:00



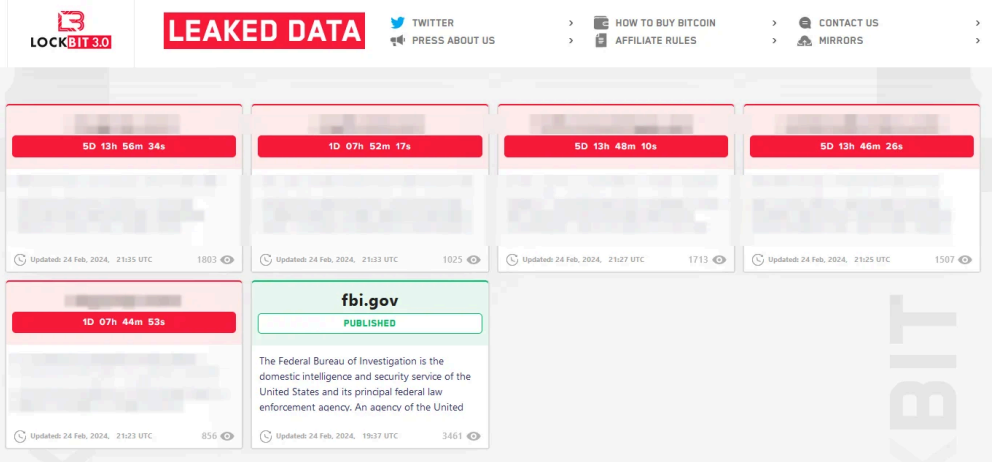
Five days later, LockBit is back and provides details about the breach and how they're going to run the business to make their infrastructure more difficult to hack.

Immediately after the takedown, the gang confirmed the breach saying that they lost only the servers running PHP and that backup systems without PHP were untouched.

On Saturday, LockBit announced it was resuming the ransomware business and released damage control communication admitting that "personal negligence and irresponsibility" led to law enforcement disrupting its activity in Operation Cronos.

The gang kept the brand name and moved its data leak site to a new .onion address that lists five victims with countdown timers for publishing stolen information.

Some of the organizations on LockBit's "leaked data" page appear to be victims of previously known attacks.



Relaunched LockBit data leak site shows five victims
source: BleepingComputer

Outdated PHP server

LockBit says that law enforcement, to which they refer collectively as the FBI, breached two main servers "because for 5 years of swimming in money I became very lazy."

"Due to my personal negligence and irresponsibility I relaxed and did not update PHP in time." The threat actor says that the victim's admin and chat panels server and the blog server were running PHP 8.1.2 and were likely hacked using a critical vulnerability tracked as CVE-2023-3824.

LockBit says they updated the PHP server and announced that they would reward anyone who finds a vulnerability in the latest version.

Speculating on the reason "the FBI" hacked their infrastructure, the cybercriminal says that it was because of the ransomware attack on Fulton County in January, which posed the risk of leaking information with "a lot of interesting things and Donald Trump's court cases that could affect the upcoming US election."

This led LockBit to believe that by attacking "the .gov sector more often" they will force "the FBI" to show if it has the ability to attack the gang.

The threat actor says that law enforcement "obtained a database, web panel sources, locker stubs that are not source as they claim and a small portion of unprotected decryptors."

Decentralized affiliate panels

During Operation Cronos, authorities collected more than 1,000 decryption keys. LockBit claims that the police obtained the keys from "unprotected decryptors" and that on the server there were almost 20,000 decryptors, about half of the

approximately 40,000 generated over the entire life of the operation.

The threat actor defines “unprotected decryptors” as builds of the file-encrypting malware that did not have the “maximum decryption protection” feature enabled, typically used by low-level affiliates that take smaller ransoms of just $2,000.

LockBit plans to upgrade security for its infrastructure and switch to manually releasing decryptors and trial file decryptions, as well as host the affiliate panel on multiple servers and provide its partners with access to different copies based on the trust level.

“Due to the separation of the panel and greater decentralization, the absence of trial decrypts in automatic mode, maximum protection of decryptors for each company, the chance of hacking will be significantly reduced” - LockBit

The long message from LockBit looks like damage control and an attempt to restore credibility for a tainted reputation.

The gang took a heavy blow and even if it managed to restore the servers affiliates have a good reason to be distrustful.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/